WHAT IS CLAIMED IS:

1. A rights management architecture for securely delivering content to authorized consumers, the architecture comprising:

a content provider;

a consumer system for requesting content from the content provider;

the content provider generating a session rights object for accessing the content;

a KDC (key distribution center) for providing authorization data to the consumer system, the authorization data for accessing the content;

a caching server for comparing information in the session rights object with the authorization data; and

the caching server forwarding the requested content to the consumer system if the information matches the authorization data.

2. The architecture of claim 1 wherein

the consumer system is redirected to the caching server to receive the requested content.

3. The architecture of claim 1 wherein the caching server and the content provider are combined into a single system identified .

4. The architecture of claim 1 wherein

the caching server employs real time streaming for securely forwarding the encrypted content.

5. The architecture of claim 1 wherein

the requested content is encrypted for forwarding to the consumer system.

6. The architecture of claim 4 wherein

the caching server and the consumer system exchange control messages for supporting transfer of the requested content.

7 . The architecture of claim 6 wherein the control messages are encrypted and authenticated.

8. The architecture of claim 5 wherein

the caching server comprises one or more cache disks for storing encrypted content.

9. The architecture of claim 5 wherein

the KDC distributes cryptographic keys, the KDC employing a blend of symmetric and public algorithms for distributing the cryptographic keys.

10. The architecture of claim 5 further comprising

a key management protocol for establishing keys between the caching server and the consumer system.

11. The architecture of claim 10 wherein the key management protocol comprises

a key request message for requesting a session key from the caching server and

responsive thereof, a key reply message for providing the session key to the consumer system.

12. The architecture of claim 11 wherein

the session rights object and the authorization data are included in the key request message;

wherein the caching server compares information in the session rights object to the authorization data; and

if the information matches the authorization data, the session key being provided to the consumer system.

13. The architecture of claim 12 wherein

the content provider generates the session rights object specifying the user's access privileges for the content.

14. A rights management method for securely delivering content upon request from a caching server, the method comprising:

providing a content provider communicably coupled to the a caching server;

providing a key management protocol comprising the steps of,

forwarding a ticket challenge message from the caching server to the content provider, the challenge message for initiating key management;

responsive thereof, sending a key request message from the content provider to the caching server;

responsive thereof, sending a key reply message from the caching server to the content provider;

responsive thereof, sending a security established message from the content provider to the caching server; and

responsive thereof, sending a security established message from the content provider to the caching server; and

establishing a set of keys for securely delivering content from the content provider to the caching server.

15. The method of claim 14 further comprising

providing a consumer system for streaming content from the caching server.

16. The method of claim 14 further comprising

providing a key distribution center for establishing trust between the caching server and the content provider.

17. A rights management method for securely pre-positioning content at a caching server, the method comprising:

providing a content provider communicably coupled to the a caching server;

providing a key management protocol comprising the steps of,

forwarding a key request message from the content provider to the caching server, the key request message for initiating key management;

responsive thereof, sending a key reply message from the caching server to the content provider; and

establishing a set of keys for securely delivering content from the content provider to the caching server.

18. The method of claim 17 further comprising

providing a consumer system for streaming content from the caching server.

19. The method of claim 17 further comprising

providing a key distribution center for establishing trust between the caching server and the content provider.

20. An authentication system allowing an authorized user to stream content from a caching server within a computing network, the system comprising:

a content provider for providing the content to the caching server for access by the user;

a key distribution center receiving from the content provider, a first request to access the caching server, and if authenticated the content provider delivers the content to the caching server; and

the key distribution center receiving from the user, a second request to access the caching server, and if authenticated the user is allowed to stream the content from the caching server.

21. The authentication system of claim 20 wherein the second request is for a caching server ticket to access the caching server.

22. A protocol for securing data transfer between components of a communication network:

a) providing a central server having a database;

b) publishing content metadata from a content provider to the central server;

c) providing a billing center server, communicably coupled to the central server;

d) reporting billing information from a caching server to the billing center server;

e)providing a provisioning database, coupled to the central server;

f) updating the provisioning database with consumer information; and

g)using a key management protocol to securely transfer data during any one or more of step b), step d), and step f).

23. The protocol of claim 22 wherein

the key management protocol comprises

forwarding a key request message for requesting a session key; and

receiving a key reply message for providing a session key.